Avaya one-X® Client Enablement Services

Release 6.1 Service Pack 3

Release Notes

Issue 1.1

30th January 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

License

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC.,ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE

USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by
End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License type(s)

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a
Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate
function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (see "Third-party Components" for more information).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit
rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and
identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright. The open source license text file, OpenSourceLicense.txt, is available in the Licenses folder on the Avaya one-X® Client Enablement Services server: /Licenses/OpenSourceLicense.txt.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Trademarks

Avaya, the Avaya logo, Avaya one-X® Client Enablement Services, Communication Manager, Modular Messaging, and Conferencing are either registered trademarks or trademarks of Avaya Inc. in the United
States of America and/or other jurisdictions. All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

Contact Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Contents

Getting Started 6

Obtaining the Avaya one-X® Mobile client application files 6

Obtaining the Avaya one-X® Communicator client release 6

Obtaining the Avaya one-X® Client Enablement Services Release 6.1 SP3 files through Avaya PLDS. 6

Obtaining the Avaya one-X® Mobile clients application files 7

Obtaining the Avaya one-X® Communicator client release 8

Installing the Avaya one-X® Client Enablement Services Release 6.1 SP3 8

Upgrading Avaya one-X® Client Enablement Services from to 6.1 SP3 (build 6.1.3.0.12) 8

Upgrading Handset Server on Standalone machine to 6.1 SP3 build 9

Verifying that IHS (IBM HTTP Server) is running post upgrade 9

Interoperability 11

Supported systems 11

Interoperability Issues 13

Client Enablement Services Release 6.1 SP3 14

Caveats 14

Fixed Issues 17

Open Issues 19

Client Enablement Services Server issues: 19

Technical Support 23

Appendix A: one-X Client Enablement Services and one-X Portal Client Interoperability 24

Appendix B: No Voicemail configuration support on one-X Client Enablement Services (workaround) ... 29

Appendix C: Converting the Handset Server configuration from Co-Resident to Standalone and vice-versa post Installation. 32

Appendix D: Acronyms 34

About Avaya one-X® Client Enablement Services

Avaya one-X® Client Enablement Services brings Unified Communications (UC) features to your desktop and mobile handsets. Client Enablement Services gives you access to multiple Avaya UC capabilities, including Telephony, Messaging, Mobility, Conferencing, and Presence services. In Client Enablement Services, the UC clients of Avaya one-X® Communicator and Avaya one-X® Mobile work with a single server. The Client Enablement Services server delivers continuous subscriber data and provides a consistent user experience.

Changes delivered as part of Client Enablement Services 6.1 Service Pack 3 release are documented here.

Getting Started

Review these notes prior to installing the Client Enablement Services 6.1 SP3 software.

Obtaining the Client Enablement Services release 6.1 SP3 files through Avaya PLDS

Obtaining the Avaya one-X® Mobile client application files

Obtaining the Avaya one-X® Communicator client release

Installing the 6.1 SP3 release of Client Enablement Services

Upgrading Client Enablement Services release to 6.1 SP3 (build 6.1.3.0.12)

Obtaining the Avaya one-X® Client Enablement Services Release 6.1 SP3 files through Avaya PLDS.

The Client Enablement Services Release 6.1 SP3 template (build number 6.1.3.0.12) will be available through the Product Licensing and Delivery System (PLDS) of Avaya.
Follow the procedure mentioned below to download and extract the template files before proceeding with the installation.

1. Select the following .tar files from the PLDS Web site and download or copy at location **/vsp-template/** of CDOM on your System Platform machine that hosts the Client Enablement Services server.
   i. oneXCES_61_3.taraa
   ii. oneXCES_61_3.tarab

iii. oneXCES_61_3.tarac
iv. oneXCES_61_3.tarad
v. oneXCES_61_3.tarae
vi. oneXCES_61_3.taraf
vii. oneXCES_61_3.tarag

2. Log in the SSH terminal of CDOM and make sure adequate (approx 13GB) disk space is available on mount **/vsp-template**. Use the **df –h** command to check space availability. You can delete the tar files and extracted files of previous build to create disk space. Do not delete the files under folder **/vsp-template/onexps_template_xxGB**, as these files are current template files used by CES.

3. Extract or untar the template files of 6.1 SP3 from the location **/vsp-template/** using the command:

```
cat oneXCES_61_3.tara* | (tar x)
```

4. This command creates the following files into a directory labeled with the version that you have downloaded, for example: /vsp-template/6.1.3.0.12:

i. backup_onexps.sh
ii. lv_rhel.img.gz
iii. onexps_template.mf
iv. onexps_template_24GB.ovf
v. onexps_template_16GB.ovf
vi. post_install.sh
vii. preweb.war
viii. restore_onexps.sh
ix. patchplugin_onexps.sh
x. versioninfo_onexps.sh

5. Use the procedure mentioned in the Implementing Avaya one-X® Client Enablement Services guide to install the template using the SP Server option.

Obtaining the Avaya one-X® Mobile clients application files

The Avaya one-X® Mobile client application files can be obtained as mentioned below.

- The Avaya one-X® Mobile 6.1 SP3 application for iPhone (build 6.1.2.0.60) can be downloaded on your iPhone from the Apple App Store.

- The Avaya one-X® Mobile 6.1.2 SP1 application for Android (build 6.1.2.205) can be downloaded on your Android device from Google Play.

- The Avaya one-X® Mobile 6.1.2 SP1 application for BlackBerry (build 6.1.2.362) can be downloaded on your BlackBerry device from BlackBerry AppWorld.

Obtaining the Avaya one-X® Communicator client release

You can obtain the Avaya one-X® Communicator client build from the Avaya PLDS site.

The following releases of Avaya one-X® Communicator client are supported with Client Enablement Services 6.1 SP3:

- Avaya one-X® Communicator R6.1 SP5

Installing the Avaya one-X® Client Enablement Services Release 6.1 SP3

The Client Enablement Services Release 6.1 SP3 can be directly installed on a new system. It does not need any prior release of the Client Enablement Services 6.1 to be present on the system.

Follow the Implementing Avaya one-X® Client Enablement Services guide for detailed instructions on installing the Client Enablement Services server.

Upgrading Avaya one-X® Client Enablement Services from to 6.1 SP3 (build 6.1.3.0.12)

If either the 6.1 GA or the 6.1 SP1/SP2 releases of Client Enablement Services is pre-installed on the system, it can be upgraded to release 6.1 SP3. Follow the procedure below to upgrade the Client Enablement Services server:

1. Copy and extract the template files of CES 6.1 SP3 at CDOM location: **/vsp-template/,** as mentioned earlier in this document.
2. Access the web console of CDOM and go to: Server Management > Backup / Restore > Backup and take the backup of the server.
3. From the web console of CDOM, go to: Virtual Machine Management > Solution Template
4. Select Install Template files from: SP server, and click Upgrade
5. Select the template of CES 6.1 SP3 build (.ovf file of same size as the one currently installed) and proceed with the upgrade
6. In the pre-install setup, all the values will be auto-populated. Verify the values, and click on Install on the last page to proceed. Do not change any values in the pre-install setup during upgrade.
7. Once the upgrade procedure reaches its completion, click on Commit to finalize the upgrade. Failing to commit will result in template roll-back to old build.

Upgrading Handset Server on Standalone machine to 6.1 SP3 build

Use following steps to upgrade the Handset server:

1. Copy the Handset Server 6.1 SP3 installable (**RHServer.bin**) from the Client Enablement Services server 6.1 SP3 location **/opt/avaya/** to the standalone machine that hosts the Handset Server.
2. Login into the Handset Server machine using SSH.
3. If you have installed any 3rd party certificates like VeriSign, ensure that you back up the IHS keystores first, and then restore the IHS keystores after the install. The keystores are located at **/opt/IBM/HTTPServer**.
   The key store at location **/opt/avaya/HandsetServer** should also be backed up.
4. Stop the currently installed Handset Server using the command: **service handset_server stop**
5. Install the 6.1 SP3 Handset Server (**RHServer.bin**) on a standalone machine. Follow the instructions as mentioned in the Implementing Avaya one-X® Client Enablement Services guide.
6. Exit the SSH terminal and re-login using SSH on the machine.
7. To verify that the Handset Server is up and running, run command:

   ps –ef | grep RoutingHandsetServer
   Handset Server process will be shown, if the server is running.
8. Stop the Handset Server using the command: **service handset_server stop**
9. Restore the keystore files.
10. Start the Handset Server using the command: **service handset_server start**
11. Restart the Handset Server services from the Client Enablement Services Web administration page.

Verifying that IHS (IBM HTTP Server) is running post upgrade

Use the following steps to verify that IHS is running after upgrade of the Client Enablement Services build.

1. For Co-resident (Handset Server) deployments:
   a. Log in using SSH on the Client Enablement Services server.
   b. To verify that IHS is up and running, run command:

ps –ef | grep HTTPServer

The system displays the IHS process ID, if the server is running.

If IHS is not running, start it using the following commands:
service ihs start and **service ihs_admin start**

2. For standalone (Handset Server) deployments:

   a. Log in using SSH on the Handset Server machine.

   b. To verify that IHS is up and running, run command:

      ps –ef | grep HTTPServer

      The system displays the IHS process ID, if the server is running.

      If IHS is not running, start it using the following commands:

      service ihs start and **service ihs_admin start**

Interoperability

Supported systems

The following table lists the supported systems by Avaya one-X® Client Enablement Services Release 6.1 SP3. This table lists the latest patch or service pack of the component that is tested with Client Enablement Services at the time of release.

Avaya Components	Supported Release
Avaya Aura® System Platform	6.0 Build 6.0.3.0.3 Patch 6.0.3.9.3
Avaya Aura® System Manager	6.1, 6.2, 6.2 FP1
Avaya Aura® Communication Manager	5.2.1, 6.0 (ES configuration only), 6.0.1, 6.2, 6.2 FP1
Avaya Aura® Session Manager	6.0, 6.1, 6.2, 6.2 FP1
Avaya Aura® Presence Services	6.1 SP2 * **any later release than above is not supported by 1XCES 6.1 SP3 (refer onexcesserver-8183 for details)*.
Avaya Aura® Messaging	6.0, 6.0.1, 6.1, 6.2
Avaya Modular Messaging	5.2
Avaya Aura® Communication Manager Messaging	6.2
Avaya Aura® Conferencing	6.0
Avaya Meeting Exchange	5.2.1
Avaya Soft Clients	Avaya one-X® Communicator – 6.1 SP5, 6.1 SP7 Avaya one-X® Mobile client for iPhone – 6.1 SP3, 6.1 SP4 Avaya one-X® Mobile client for Android – 6.1.2 SP1, 6.1 SP4 Avaya one-X® Mobile client for BlackBerry – 6.1.2 SP1
Avaya one-X® Portal	5.2

Note – CES supports integration with Avaya Aura 6.2 FP1 setup; however Presence functionality would be unavailable due to issue onexcesserver-8183. To continue using the Presence functionality, PS release must be 6.1 SP2.

3rd Party Components	Software / Hardware	Supported Release / Model
CES Server OS	Linux	RHEL (part of the System Platform template)
Handet Server OS	Linux	RHEL 5.8
LDAPs	Microsoft Active Directory	2003 R2, 2008 R2
	Microsoft ADAM / AD LDS	2003 / 2008
	IBM Domino Server	8.5.3
	Sun Java System Directory Server Enterprise Edition	6.3.1, 7.0
	Novell e-Directory	8.8 SP7
CES Administration Browser	Microsoft Internet Explorer	7.0, 8.0
	Mozilla Firefox	3.6
	Apple Safari	5.x
Mobile Device Platforms	iPhone (Apple)	4.3+, 5.0, 6.0
	BlackBerry (RIM)	5.0+, 6.0+, 7.0
	Android	2.2+, 4.0
Mobile Devices	iPhone (Apple)	3G, 3GS, 4, and 4S
	BlackBerry (RIM)	Bold – 9650, 97xx, 9000, 99xx Storm – 9550 Curve – 8520 , 8530, 8900, 9300 Torch – 9800
	Android	Motorola - Droid 2, A953, Atrix4G. HTC –MyTouch 4G, Desire HD, Desire S, EVO 4G. LG – Revolution, Optimus 3D. Samsung – Galaxy, Galaxy S, Galaxy SII, Nexus Dell – Venue

Interoperability Issues

Known interoperability issues with Client Enablement Services 6.1 SP3:

Interop Component	Interop Issue ID	Problem	Workaround / Notes
Avaya Aura® Communication Manager	defsw103257	No visual or audio alert on the desk phone of a SIP station if it is configured for silent ringing (ONEXCESSERVER-6063).	
	defsw122036	Call logs on 1xM will be shown with "NO SUBJECT" or "UNKNOWN" when make a callback from 1xM via H.323 Deskphone to another station (ONEXCESSERVER-8152).	
Avaya Aura® Messaging	MSG-2422	Client Message details window incorrectly shows priority tag on it after reading it (wi00888102). Note – If SMS Notification is enabled for Priority VMs, then no SMS Notification is received on the Avaya one-X® Mobile clients for priority VMs (ONEXCESSERVER-7517).	This would be addressed in Avaya Aura® Messaging 6.3 release.

Changes delivered to Avaya one-X® Client Enablement Services Release 6.1 SP3

Client Enablement Services Release 6.1 SP3

The Client Enablement Services 6.1 SP3 includes new defect fixes in addition to the fixes delivered as part of Client Enablement Services 6.1 SP2 release.

Client Enablement Services 6.1 SP3 now also supports a new LDAP type integration with Microsoft Active Directory Application Mode (ADAM) 2003 and Microsoft Active Directory Lightweight Directory Services (AD LDS) 2008.

Interoperability support with Avaya Aura® Communication Manager Messaging as Voice Messaging server and Avaya Aura 6.2 is added in Client Enablement Services 6.1 SP3.

The default certificate in Client Enablement Services 6.1 SP3 is signed by Avaya CA.

Caveats

Fixed Issues

Open Issues

Caveats

Avaya one-X® Client Enablement Services Release 6.1 SP3 has following caveats:

one-X CES ID	Caveat	Workarounds/Notes
Client Enablement Services Server Administration -		
NA	Client functionalities would be impaired if same user is configured for both Avaya one-X Mobile server 5.2 and Client Enablement Services.	Do not configure Avaya one-X Mobile server 5.2 and Client Enablement Services for the same user (extension) on Communication Manager.
NA	Client Enablement Services does not support configurations where a managed user is not part of the corporate directory. Furthermore, a unique handle or userid is required for users.	All Client Enablement Services users must be part of the corporate LDAP directory.

one-X CES ID	Caveat	Workarounds/Notes
	Note – the handle or userid should not have any space in it.	
NA	Client Enablement Services does not support user configurations that do not have voicemail setup.	Assign voicemail resource when provisioning the user from web administration application. Refer to the Appendix at the end of this document for implementing a workaround to provision users with no voicemail setup.
NA	Client Enablement Services do not support multiple direct SIP trunks from the same Client Enablement Services Server to the same Communication Manager server.	Configure only one direct SIP trunk between Client Enablement Services and Communication Manager.
NA	Cannot save Notification server information using Client Enablement Services web admin console if the SMTP server is not reachable (IP and Port)	IP and Port should be reachable while adding SMTP details
Client Enablement Services Client Features -		
NA	Messaging – VM of length up to 7 minutes supported and could be downloaded and played on mobile client.	None.
NA	Messaging – Mobile users can have maximum of 15 voice messages available on their mobile application.	Delete displayed voice messages to see other VMs in the queue.
NA	CMM Messaging – CMM is low capacity voice messaging system; therefore, the voicemails updates received via CMM are relatively slower as compared to other messaging systems like Modular Messaging or Avaya Aura Messaging.	None.
NA	Call Handling – DTMF Prompt on client sounds like a	When DTMF is enabled for an end user on the Client Enablement

one-X CES ID	Caveat	Workarounds/Notes
	dial tone	Services, the end user hears a dial tone. This is Communication Manager prompting the user to press a key for confirmed answer of inbound or callback calls.
NA	Call Handling – Extend Call button on the Desk Phone only works if the user has the mobile phone set to ring. Call will not be extended to other Ring Also phones.	Set Mobile Phone to ring for Extend Call feature to work from Desk Phone.
NA	Call Handling – Auto-answer set on the user's extension will not work if the extension is controlled by Client Enablement Services.	None.
NA	Call Handling – Send All Calls (SAC) feature on Desk Phone and Block All Calls (BAC) feature on one-X client are not the same and not in sync. Activating / deactivating SAC would not activate / deactivate BAC and vice-versa.	It is recommended that user use one-X client to activate / deactivate Block All Calls and not use SAC feature on Desk Phone for sending incoming calls to coverage.
ONEXCESSERVER-6415	Callback – In the event of the user being a SIP endpoint, the user has to accept the call at the desk-phone to complete a callback call if the origination point of the call is selected as the desk-phone	Upgrade the firmware on the SIP Hard-Phone that is being used as the deskphone. (firmware versions 2.6.7.0. and above).
NA	Ring Also / Callback – On-PBX extensions (internal destinations), except own extension, are not supported as Also Ring or Callback origination phones.	None.

one-X CES ID	Caveat	Workarounds/Notes
NA	Ring Also – Client Enablement Services does not support configurations where two users add the same mobile number as their Ring Also destination.	All users should have unique mobile number as their Ring Also destination.
ONEXCESSERVER-6920	Ring Also – No option for enable/disable ringing at Also Ring phones for calls on bridge-call-appearance.	This would be available in CES 6.2 release.

Fixed Issues

Following issues are fixed in Client Enablement Services Release 6.1 SP3:

Issue ID	Issue Description	Notes
Server Administration -		
ONEXCESSERVER-7972	Handset Server stops abruptly with the exception "java.lang.OutOfMemoryError:"	Fixed.
ONEXCESSERVER-8089	Handset Server (HS) restarts intermittently.	Fixed.
ONEXCESSERVER-7278	javax.servlet.sip.TooManyHopsException is seen on the Client Enablement Services system if it is integrated with Session Manger over TLS. This might result in collection of heap dumps on the Client Enablement Services system.	Fixed.
ONEXCESSERVER-7339	Heap dumps are collected at regular intervals on some Client Enablement Services systems resulting in 100% disk space utilization on the template and disrupting the services.	Fixed.

Issue ID	Issue Description	Notes
ONEXCESSERVER-7850	CES Server Failure - System down. Web Admin Core ERROR	Fixed.
ONEXCESSERVER-8150	SSL weak encryption vulnerability.	Fixed.
ONEXCESSERVER-7929	The script for importing, exporting user data and managing keys (1xpAdmin.sh) fails from remote Linux or Windows system.	Users' data can now be managed from remote machines.
ONEXCESSERVER-7587	Unable to delete a disabled user from the provisioned users' page on 1XCES web admin.	Fixed.
Client Enablement Services Client Features -		
ONEXCESSERVER-7592	Presence status not available for Favorite Contacts on 1XM client.	Fixed.
ONEXCESSERVER-8084	LDAP DN is shown as Display Name on 1XC when integrated with LDAP type ADAM.	User name is now displayed on the client.
ONEXCESSERVER-8105	ADAM Integration: LDAP DNs are displayed instead of Names as a part of search results on 1XC in 1XCES integration mode.	User names are now displayed on the client.
ONEXCESSERVER-8384	Call icon not appearing on 1xC for voicemail left when MM mailbox Subscriber calls - CES/MM enabled user.	Fixed.
ONEXCESSERVER-8376	[Intermittent] Multiple outbound calls are initiated from Bridge Conference dial out UI on 1XC client.	Fixed.
ONEXCESSERVER-8249	Not able to add participant to the Bridge Conference using MX moderator codes *1 to dial out then *2 to add/join new participant on 1XC client.	Fixed.

Open Issues

The following issues will be addressed in a future release. This 6.1 SP3 Release includes the following known issues in Client Enablement Services:

Client Enablement Services Server issues:

Issue ID	Problem	Workaround/Notes
Installation and Upgrade -		
ONEXCESSERVER-7157	Service account password with $ does not install CES properly and throws error when accessing web admin.	Do not use $ in the service account password.
ONEXCESSERVER-7184	[upgrade] IHS dmz host not configured after upgrade	Update the dmz host in the /opt/avaya/1xp/config.properites file and then run the run_config_httpservers_jython.pl run. Refer the Implementing Avaya one-X® Client Enablement Services guide for details.
NA	[upgrade] Messaging certificates not retrieved post upgrade and non-default Messages Temp Directory value not retained.	Manually retrieve the Messaging certificates and enter the Temp Directory using Client Enablement Services Web administration application. Refer Administering Avaya one-X® Client Enablement Services guide for details.
ONEXCESSERVER-8322	After a fresh installation, "service handset_server status" shows HS as running while "ps -ef |grep Handset " gives no process of Handset running	After restarting HS process, the handset server status is shown correctly.
ONEXCESSERVER-7508	Audio Transcoding page on Monitors shows Exception in Internal Client API post fresh install of CES	Restart WAS after installing CES.
ONEXCESSERVER-8256	SIP Local Port and Secure option is not retained after upgrading from CES 6.1 SP2 to 6.1 SP3	Manually update the settings post upgrade.
Administration -		
ONEXCESSERVER -7212	DB backup when initiated from Client Enablement Services web admin would fail if sufficient disk space is not available for storage of the	Always move the backup files to a remote storage server and keep sufficient disk space available for future db backups.

Issue ID	Problem	Workaround/Notes
	backup files.	Refer to the Administering guide for details on managing disk space.
ONEXCESSERVER-7488	1XCES web admin not accessible using service account post LDAP restart.	Restart 1XCES (WAS) services.
ONEXCESSERVER-6847	On the one-X CES server when the "UserID" Attribute is modified to "userPrincipleName" on the "Modify LDAP Attribute" page, then post enterprise directory sync, login fails from clients.	Do not change this setting.
ONEXCESSERVER-7110	User part of the Audit group is able to logoff and kill active sessions of a provisioned user.	None.
ONEXCESSERVER-7757	Deleting the user/re-provisioning the user not clearing out the user information.	Restart User Assistant service from 1XCES web admin to fix this.
ONEXCESSERVER-7885	CM does not always release the ONE-X licenses when WAS is stopped or the CES template is stopped form the CDOM.	Run the Command “System Reset 4” on the CM to flush any redundant ONE-X license usage.
ONEXCESSERVER-7531	Mobile resource for a user added via admin does not validate the route	Make sure the Mobile number added is routable through CM.
ONEXCESSERVER-8178	MM adapter is still shown in connected state when Voice Messaging server is completely stopped.	Restarting the MM adapter will get the state reflected correctly.
ONEXCESSERVER-7509	Presence adapter does not connect immediately when added.	Restart the PS adapter from 1XCES web admin > Monitor > Presence page.
ONEXCESSERVER-8183	Presence adapter does not connect when integrated with PS 6.1.5 (FP1 release).	CES 6.1 SP3 does not support PS 6.1.5 or later. This will be fixed in CES 6.2.
ONEXCESSERVER-8245	Launching Handset page using auditor account causes exception	Using admin account instead to access the Handset Server page on CES web admin.

Issue ID	Problem	Workaround/Notes
ONEXCESSERVER-7326	1XCES server IP sent in the 2nd Notification SMS in Standalone HS deployments instead of the HS server.	None.
ONEXCESSERVER-8223	[Intermittent] Unable to delete user from 1XCES web admin.	Restart 1XCES (WAS) services.
Client Enablement Services Client Features -		
ONEXCESSERVER-5914	Email2 shown for Contacts when both Email1 and Email2 are configured for users on LDAP.	Do not use different email addresses. In LDAP Attribute Mappings change E-mail 2 attribute to otherMailbox (instead of proxy address).
ONEXCESSERVER-8408	VM are not shown on the Mobile (1XM) client after setting the VM PIN post login.	Re-login on the 1XM client after setting the VM PIN.
ONEXCESSERVER-8345	Number to name resolution does not work for CMM Messaging.	None.
ONEXCESSERVER -8300	[Intermittent] Call logs are deleted from 1XC but they are still displayed on 1XM client of same user.	Re-login on 1XM client to reflect the updated call logs.
ONEXCESSERVER-7870	Maximum Number of Favorites value set in the System/Group Profile is not reflected on the Mobile (1XM) client.	None.
ONEXCESSERVER-7996	If presence note set on 1XM, note cannot be over-ridden by 1XC or Flare users.	None.
ONEXCESSERVER-7523	Presence state not displayed properly on Client If the user's username and E-mail attribute are not the same.	None.
ONEXCESSERVER -8374	Moderator unable remove any of participants on bridge conference using dial out sequence (*2) and Extension number of user not show on UI bridge conference when added using dial out feature (*1) from 1XC client.	Add users from the 1XC Client using the options provided on the UI. Moderator would then be able to control these users.

Issue ID	Problem	Workaround/Notes
ONEXCESSERVER-6768	Active call (callback call) on Mobile dropped is when new number is added in Ring Phones list via the 1XM client.	Do not edit ring phones while on a call.
ONEXCESSERVER -8378	[Intermittent] Users are removed from conference by moderator when clicked on “Remove from Conference” on 1XC client UI, but they are still displayed on UI conference bridge of 1XC client.	None.

Technical Support

Support for Client Enablement Services is available through the normal Avaya escalation process. If you encounter trouble with Client Enablement Services:

1. Retry the action. Follow the instructions in written or online documentation carefully.
2. Check the documentation that came with your hardware for maintenance or hardware-related problems.
3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.
4. If you continue to have a problem, submit a trouble ticket to Avaya.

When you request technical support, provide the following information:

- Configuration settings
- Usage scenario, including all steps required to reproduce the issue.
- Screenshots, if the issue occurs in the Administration Application, end-user web site or mobile clients.
- Copies of all logs related to the issue.
- All other information that you gathered when you attempted to resolve the issue.

Appendix A: one-X Client Enablement Services and one-X Portal Client Interoperability

Abstract

This section outlines the user provisioning and test results of interoperability when a single user (same extension on Communication Manager) uses the Avaya one-X Portal 5.2 client with Avaya one-X® Client Enablement Services 6.1 clients.

The scope of this interoperability testing includes:

- Telephony
- History
- Presence
- Messaging and other product functionalities across 1XP and 1XCES clients.

Test Environment Details

Components	**Release**
Avaya one-X Portal	5.2 SP4
Avaya one-X Client Enablement Services	6.1 SP1
Communication Manager	6.0.1 SP6
Application Enablement Services	6.1
Presence Services	6.1
Intelligent Presence Services	1.0 SP2
Session Manager	6.1 SP4
System Manager	6.1 SP4
Conferencing	6.0
Messaging	6.0.1
LDAP	Microsoft Active Directory 2008

Note – For Presence functionality, one-X Portal 5.2 server supports integration with IPS 1.0 and one-X Client Enablement Services 6.1 supports integration with PS 6.1. Both IPS 1.0 and PS6.1 are needed in the environment if Presence interop is required between 1XP and 1XCES clients.

However, there are certain limitations in the Presence interop between 1XP and 1XCES clients, which are listed in below sections.

Client Details

For one-X Client Enablement Services, following clients are used -

Avaya one-X mobile client (1XM)	Version: 6.1 SP1	Platform: iOS client for iPhone
Avaya one-X Communicator client (1XC)	Version: 6.1 SP3	Platform: Windows XP

For one-X Portal, following client is used -

Portal client (1XP) for Avaya one-X Portal	Version: 5.2.4	Platform: IE 8 on Win 7 and XP

Note – The user has H.323 extension associated on the Communication Manager. one-X Portal 5.2 does not support SIP users.

User Provisioning and Login:

- <u>1XCES 6.1 (for 1XM, 1XC clients)</u>:
    - Corporate user is provisioned on one-X Client Enablement Services 6.1
    - User logs-in using one-X mobile client connected to the one-X Client Enablement Services 6.1
    - The user can also login using one-X Communicator client connected to the one-X Client Enablement Services (using My Computer, Specify Other or Desk phone modes)

- <u>1XP 5.2 (for 1XP client)</u>:

- Same corporate user is provisioned on the one-X Portal 5.2 server
- Mobility must be **disabled** for this user on the one-X Portal during provisioning, and no EC500 mapping for the user's mobile must be configured on the Communication Manager.
- User logs-in using Portal client connected to the one-X Portal (using My Computer, Specify Other or Desk phone modes)

High level test observations

Area	**Observation**
Login	Login into 1XP, 1XC and 1XM clients is working.
	Limitation: User must be logged into only one of the desktop clients at a time – 1XP or 1XC. If user wants to switch between the clients, he should first log off from the active client and then login into the other client. User can simultaneously login into the 1XM client with 1XP or 1XC client.
Call Handling	Call handling using same user when logged in on 1XP / 1XC and 1XM is working. Mid-call handling like Conference, Transfer, Mute, Hold/Resume, etc is working from 1XP or 1XC clients.
History	Call history / logs for same user are in sync on 1XP / 1XC and 1XM clients.
	Limitation: If user is logged off from 1XP client and he makes/receives some calls using the desk phone or other clients, these entries are not reflected in call logs displayed on 1XP client. This feature is not supported in one-X Portal 5.2 release.
Presence	Telephony Presence updates (BUSY state on active call) are seen on 1XP / 1XC and 1XM clients.
	Limitation: User Defined (manual) Presence state is **not** reflected across 1XP and 1XCES (1XM/1XC) when set either on 1XP or on 1XCES clients.

	However, the User Defined (manual) Presence state is updated between 1XM and 1XC when set on either of these clients.
Messages	Voice messages are synced correctly across 1XP / 1XC and 1XM clients.
Bridge Conferencing	Bridge Conferencing works on 1XP / 1XC clients.
Contacts / Favorites	Enterprise search is working on 1XP / 1XC and 1XM clients.
	Limitation: Contacts added as Favorites on 1XP client are not reflected on 1XCES clients (1XM and 1XC) and vice-versa.
Block All Calls / DND	Block All Calls works from 1XM and 1XC clients. DND works from 1XP clients.
	Limitation: Activating Block Calls (BAC) on 1XM or 1XC does **not** activate DND on 1XP client. Calls are sent to coverage when BAC is activated. Activating DND on 1XP client does **not** activate BAC on 1XM or 1XC clients. Calls are send to coverage when DND is activated. BAC / DND must be deactivated using the client (1XP or 1XCES) from where it is activated.
VIP Calling	VIP Calling works from 1XC and 1XM clients.
	Limitation: 1XP client does not support VIP Calling.
Ring Also	Ring Also, Silent Ringing functionalities are working using 1XM, 1XC clients.
	Limitation: Ring Also (EC500 Mobility) must be **disabled** for 1XP client to avoid conflict with 1XCES client Ring Also settings. The user won’t have control over Mobility settings using 1XP client.

Other observations

When there are different users (with different extensions on Communication Manager) using 1XP and 1XCES clients, there are certain limitations and configurations that are needed for the Presence functionality to work between the users –

1. To see the Presence state of 1XCES user on 1XP client, the 1XCES user has to be provisioned on 1XP. Else the Presence state of the 1XCES user will be shown as Offline on 1XP client.
2. The Presence reflected across 1XP and 1XCES clients is Automatic Telephone Presence (BUSY state on active call). No user defined / manual Presence is reflected across the clients.

Rest of the functionalities work as expected.

Appendix B: No Voicemail configuration support on one-X Client Enablement Services (workaround)

Abstract

Currently, the Client Enablement Services do not support user configuration without voicemail integration. However, to enable users to use other features of Client Enablement Services in such environment, a temporary workaround is available while provisioning the users on the Client Enablement Services and is outlined in this section.

Test environment, provisioning details and relevant test observations in such configuration are included.

Test Environment Details

Components	**Release**
Avaya one-X Client Enablement Services	6.1 SP1
Communication Manager	6.0.1
Presence Services	6.1
Session Manager	6.1
System Manager	6.1
LDAP	Microsoft Active Directory 2008

Client Details

Following clients are certified to support this no-VM configuration -

Avaya one-X mobile client (1XM)	Version: 6.1 SP1 (6.1.0.0.49)	Platform: iPhone Client
Avaya one-X mobile client (1XM)	Version: 6.1 SP1 (6.1.1.010)	Platform: BlackBerry Client
Avaya one-X mobile client (1XM)	Version: 6.1 SP1 (6.1.418)	Platform: Android Client
Avaya one-X Communicator client (1XC)	Version: 6.1 SP3 (6.1.3.10)	Platform: Windows XP

User Provisioning on Client Enablement Services:

Following configuration is required on the Client Enablement Services to support this workaround -

- While provisioning the users through web admin, click to **Add** the Voice Messaging resource (note that this is required, even if Messaging is not integrated with Client Enablement Services or not available for that user).
- On the Add Resource (Voice Messaging) page, leave the Server field as **<NO SERVER>**
- Provide a name of the resource in field "**Display Name**".
- Do not enter any other information and click **OK** to add this resource for the user.
- Proceed to add other resources that are required for this user and then click on **Finished** to Save the configuration.

Note – This configuration is not available when provisioning users through CLI.

Some relevant test observations on no-VM configuration users –

Test Area -	Login
iPhone and BlackBerry Mobile Client	User login works. Prompts for Mobile Account Setup on 1st login, no prompt for VM PIN.
Android Mobile Client	User login works. When the user logs in for the 1st time, the app prompts for Mobile Account Setup, no prompt for VM PIN. On completing this setup, the app exits. User has to re-launch the app to start using it.
1XC Windows Client	Login works with Client Enablement Services integration

Test Area -	Block Calls
iPhone, BlackBerry and Android Mobile Client	When Block All Calls is activated, the callers get a reorder tone if the coverage path is not defined on the user's extension on Communication Manager. When Allow VIP Calls is activated, the non-VIP calls land on the deskphone of the user, but are not sent to the Ring Also phones if

	coverage path is not defined on the user's extension on Communication Manager. VIP calls are sent to the deskphone and to the Ring Also phones, if any.
1XC Windows Client	When Block All Calls is activated, incoming calls will ring on the 1XC client silently if the coverage path is not defined on the user's extension on Communication Manager. When Allow VIP Calls is activated, incoming calls from non-VIP will ring on the 1XC client silently if the coverage path is not defined on the user's extension on Communication Manager. VIP calls ring normally on 1XC and on the Ring Also phones, if any.

Test Area -	Settings
iPhone, BlackBerry and Android Mobile Client	Following Settings would not be applicable on the mobile clients and would return error or not work as expected when edited through the clients, hence should not be edited – 1. Corporate Voicemail 2. Message Notification 3. Voicemail PIN
1XC Windows Client	Messaging settings would not be applicable on the 1XC client and would not work as expected, hence should not be edited.

Test Area -	Speech Access
iPhone, BlackBerry and Android Mobile Client	Speech Access to Messaging would not work if Messaging system is not integrated with Client Enablement Services.

Note –

1. All Messaging related features on the Mobile and Communicator clients would not work.
2. Apart from the ones mentioned above, all other functionalities of the Client Enablement Services clients and the server works as expected.

Appendix C: Converting the Handset Server configuration from Co-Resident to Standalone and vice-versa post Installation.

Abstract

Currently the Handset server configuration i.e., either co-resident or standalone has to be selected at the time of 1xCES template installation. You cannot revert this selection post installation.

This section provides the necessary steps to change the configuration of the Handset Server either from the Co-resident installation to Standalone or vice versa post the installation of the Avaya one-X® Client Enablement Services template.

A. Converting a Co-resident Configuration to a Standalone Configuration.

Current Configuration – Co-resident (the Client Enablement Server and Handset Server are on the same hardware.)
Desired Configuration – Standalone (the Client Enablement Server and Handset Server are on different hardware).

Procedure –

Step 1 On the Co-resident CES server machine, stop the Handset Server using the command: **service handset_server stop**

Step 2 Ensure that the handset server is properly stopped. Run the command: **ps –ef | grep RoutingHandsetServer**.
There should be no process id corresponding to this process

Step 3 Disable the service on the co-resident machine using the following commands:
chkconfig handset_server off
chkconfig handset_server --del

Step 4 Rename the folder ***/opt/Avaya/HandsetServer*** on the Avaya one-X® CES machine to a temporary name.
For example, ***mv /opt/Avaya/HandsetServer /opt/Avaya/HandsetServer_temp***

Step 5 Log in to the admin portal of the Avaya one-X® CES machine and navigate to Servers -> Handset -> change the IP Address of the Handset Server to that of the standalone Handset server machine and save the page.

Step 6 Restart the WAS by running the following command on the CLI of the Avaya one-X® CES server **service 1xp restart**
When prompted enter the admin username and password.

Step 7 Install the Handset Server on the standalone machine. Installation steps are present in the Implementing Client Enablement Services guide.

Step 8 Post Installation copy the certificate files, keystore.jks, from the Handset Server machine to the following location on the Avaya one-X® CES Server machine ***/opt/IBM/WebSphere/AppServer70/lib/ext/***

Step 9 Restart the Handset Services from the Avaya one-X® CES server web admin portal. Navigate to Monitors -> Handset -> Click Restart.

Step 10 Restart the Handset Server from the standalone machine using the command: **service handset_server restart**

Step 11 Once the Handset Server comes up, the users can now use this Handset Server IP or FQDN to login into the Mobile clients.

B. Converting a Standalone Configuration to a Co-resident configuration.

Current Configuration – Standalone (the Client Enablement Server and Handset Server are on different hardware.)
Desired Configuration – Co-resident (the Client Enablement Server and Handset Server are on the same hardware.)

Step 1 Log in to the CLI of the Standalone Handset Server and delete the Handset Server. Steps are present in the Administering Avaya one-X® Client Enablement Service guide.

Step2 Log in to CLI of the Avaya one-X® CES server machine as a root user and stop the WAS by using the command **service 1xp stop**
When prompted enter the admin username and password.

Step 3 On the CLI of the Avaya one-X® CES Server machine, navigate to ***/opt/avaya/*** **RHServer.bin** file is present in that folder.

Step4 Install the Handset server on the Avaya one-X® CES Server machine. Steps are present in the Implementing Client Enablement Services guide.

Step 6 Start the WAS by using the command: **service 1xp start**

Step 7 Once the server comes up, log in to the web portal of the Avaya one-X® CES Server and navigate to Servers -> Handset -> change the IP Address of the Handset Server to the local machine IP.

Step8 Restart the Handset Services from the Avaya one-X® CES Server web admin portal. Navigate to Monitors -> Handset -> Click Restart.

Step 9 Restart the Handset Server from the Avaya one-X® CES Server machine using the command: **service handset_server restart**

Step 10 Once the Handset Server comes up, the users can now use this Handset Server IP or FQDN to login into the Mobile clients.

Appendix D: Acronyms

HS	Handset Server
1XM	Avaya one-X® Mobile client
1XC	Avaya one-X® Communicator client
1XP	Avaya one-X® Portal client
1XCES/one-X CES	Avaya one-X® Client Enablement Services
CM	Avaya Aura® Communication Manager
CMM	Avaya Aura® Communication Manager Messaging
SMGR	Avaya Aura® System Manger
AES	Avaya Application Enablement Server
PS	Avaya Aura® Presence Services
SP	Service Pack
AD	Microsoft Active Directory
ADAM	Microsoft Active Directory Application Mode
AD LDS	Microsoft Active Directory Lightweight Directory Servi ces